2000.054500/DIR
TT4051

Application for United States Letters Patent

for

SOFTWARE MODEM WITH PRIVILEGED MODE OVERSIGHT OF CONTROL PARAMETERS

by

David W. Smith

Brian C. Barnes

Terry L. Cole

Rodney Schmidt

Geoffrey S. Strongin

and

Michael Barclay

EXPRESS MAIL MAILING LABEL

NUMBER EL798365418US

DATE OF DEPOSIT 9 July, 2001

I hereby certify that this paper or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington D.C. 20231

Signature

SOFTWARE MODEM WITH PRIVILEGED MODE OVERSIGHT OF CONTROL PARAMETERS

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

This invention relates generally to modem communications and, more particularly, to a software modem with privileged mode oversight of control parameters.

2. DESCRIPTION OF THE RELATED ART

In recent years cellular telephones have become increasingly popular. A cellular telephone is one example of what is referred to as a "mobile station" or "mobile terminal." A mobile station can take on various forms other than a cellular telephone, including a computer (e.g., a notebook computer) with mobile communication capabilities.

Telecommunications services are provided between a cellular telecommunications network and a mobile station over an air interface, *e.g.*, over radio frequencies. Typically, each subscriber having a mobile station is assigned a unique International Mobile Subscriber Identity (IMSI). At any moment, an active mobile station may be in communication over the air interface with one or more base stations. The base stations are, in turn, managed by base station controllers, also known as radio network controllers. A base station controller together with its base stations comprise a base station system. The base station controllers of a base station system are connected via control nodes to a core telecommunications network, such as the publicly switched telephone network (PSTN). One type of standardized mobile telecommunications scheme is the Global System for Mobile communications (GSM). GSM includes standards that specify functions and interfaces for various types of services. GSM systems may be used for transmitting both voice and data signals.

A particular base station may be shared among multiple mobile stations. Because the radio spectrum is a limited resource, the bandwidth is divided using combination of Time-Division and Frequency-Division Multiple Access (TDMA/FDMA). FDMA involves dividing the maximum frequency bandwidth (*e.g.*, 25 MHz) into 124 carrier frequencies spaced 200 kHz apart. A particular base station may be assigned one or more carrier frequencies. Each carrier frequency is, in turn, divided into time slots. During an active session between the base station and the mobile station, the base station assigns the mobile unit a frequency, a power level, and a time slot for upstream transmissions from the mobile station to the base station. The base station also communicates a particular frequency and time slot for downstream transmissions from the base station destined for the mobile station.

The fundamental unit of time defined in GSM is referred to as a burst period, which lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a TDMA frame (120/26 ms, or approx. 4.615 ms), which is the basic unit for the definition of logical channels. One physical channel is defined as one burst period per frame. Individual channels are defined by the number and position of their corresponding burst periods.

GSM frames, each frame having 8 burst periods, are grouped into superframes (*e.g.*, groups of 51 frames) that include both traffic (*i.e.*, voice or data signals) and control information. The control information is conveyed over common channels defined in the superframe structure. Common channels can be accessed both by idle mode and dedicated mode mobile stations. The common channels are used by idle mode mobile stations to exchange signaling information for changing to dedicated mode in response to incoming or outgoing calls. Mobile stations already in the dedicated mode monitor the surrounding base stations for handover and other information.

The common channels include:

a Broadcast Control Channel (BCCH) used to continually broadcasts information including the base station identity, frequency allocations, and frequency-hopping sequences;

a Frequency Correction Channel (FCCH) and Synchronization Channel (SCH) used to synchronize the mobile station to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering (*i.e.*, every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are, by definition, sent on time slot number 0 within a TDMA frame);

a Random Access Channel (RACH) used by the mobile station to request access to the network;

a Paging Channel (PCH) used to alert the mobile station of an incoming call; and

an Access Grant Channel (AGCH) used to allocate a Stand-alone Dedicated Control Channel (SDCCH) to a mobile station for signaling (*i.e.*, to obtain a dedicated channel) following a request on the RACH.

For security reasons, GSM data is transmitted in an encrypted form. Because a wireless medium can be accessed by anyone, authentication is a significant element of a mobile network. Authentication involves both the mobile station and the base station. A Subscriber Identification Module (SIM) card is installed in each mobile station. Each subscriber is assigned a secret key. One copy of the secret key is stored in the SIM card, and another copy is stored in a protected database on the communications network that may be

accessed by the base station. During an authentication event, the base station generates a random number that it sends to the mobile station. The mobile station uses a random number, in conjunction with the secret key and a ciphering algorithm (*e.g.*, A3), to generate a signed response that is sent back to the base station. If the signed response sent by the mobile station matches the one calculated by network, the subscriber is authenticated. The base station encrypts data transmitted to the mobile station using the secret key. Similarly, the mobile station encrypts data it transmits to the base station using the secret key. After a transmission received by the mobile station is decrypted, various control information, including the assigned power level, frequency, and time slot for a particular mobile station may be determined by the mobile station.

Generally, communication systems are described in terms of layers. The first layer, responsible for the actual transmission of a data carrying signal across the transmission medium, is referred to as the physical layer (PHY). The physical layer groups digital data and generates a modulated waveform based on the data in accordance with the particular transmission scheme. In GSM, the physical layer generates the transmission waveform and transmits during the assigned transmit time slot of the mobile station. Similarly, the receiving portion of the physical layer identifies data destined for the mobile station during the assigned receipt time slot.

The second layer, referred to as a protocol layer, processes digital data received by the physical layer to identify information contained therein. For example, in a GSM system, decryption of the data is a protocol layer function. Notice that changes in the operating parameters of the physical layer are identified only after decryption and processing by the protocol layer. Although this particular interdependency does not generally cause a problem

in a purely hardware implementation, it may cause a problem when all or portions of the protocol layer are implemented in software.

Certain computer systems, especially portable notebook computers, may be equipped with wireless modems. One trend in modem technology involves the use of software modems that implement some of the real-time functions of traditional hardware modems using software routines. Because the hardware complexity of a software modem is less than a hardware counterpart, it is generally less expensive as well as more flexible. For example, the protocol layer decryption and processing may be implemented partially or entirely with software.

Software systems, such as PC systems, run interface control software in operating systems environments as software drivers. These drivers are responsible for communicating to the hardware devices and operate at a privileged level in the operating system. Other software applications are precluded from affecting the drivers. However, because drivers are not protected from other drivers, a variety of problems can occur that might affect the operation of a driver, such as by corrupting its operation. These effects may be caused accidentally, or may be caused by purposeful hacking. A corrupted (or co-opted) driver might cause additional problems outside the computer, such as causing a phone line or wireless channel to be used, operating an external peripheral, or deleting important data.

Because the operating parameters of the physical layer, which control the operation of the transmitter of the mobile station, are controlled by the protocol layer using software, it may be possible for a computer program or virus to take control of the mobile station and cause it to accidentally or purposefully transmit outside of its assigned time slot. A wireless communications network, such as a cellular network, relies on a shared infrastructure. A

10050711 .035701

mobile station must adhere to the 'rules of the road' or it may cause interference on the network.

If certain functions of the mobile station are controlled in software, a programmer may determine how the GSM control frames are decoded and how the transmitter module is triggered. A virus may then be written and spread over the network to infiltrate the software-based mobile stations. Then, on a particular time and date, the virus could take direct control of the mobile station and transmit continuously or intermittently and inundate the base stations and other mobile units with random frequencies and full power. Such a virus design could enable and disable at random times to avoid detection, robbing the air-time supplier of some or all of his available bandwidth and may even cause a complete shutdown of the network. Such an attack may take only a few affected devices (*i.e.*, as few as one) per cell to disable the cell completely.

The security problems associated with mobile stations operating in a shared infrastructure may be segregated into three levels of severity: tamper-proof, non-tamperproof, and class break. First, a hardware/firmware implementation (such as a cell-phone) is the hardest with which to tamper, because each device must be acquired individually and modified (*i.e.*, tamper-proof). On the other hand, a software-based solution is easier to tamper with, as a hacker can concentrate on a software-only debugger environment (*i.e.*, non-tamper-proof). Finally, a system with the ability to be tampered with that is similar on all systems and allows the tampering to be distributed to a large number of systems of the same type is susceptible to a 'class-break.'

A software wireless modem is susceptible not only to a class-break, but also it is among those devices whose code may be accessed from the same layer as IP (internet protocol) or another portable code access mechanism. Many software wireless modems may

be integrated into computers coupled to networks or the Internet. Such an arrangement increases the susceptibility of the software to being tampered with and controlled.

Communication devices implementing other communications protocols using software may also be susceptible to some of the problems identified above, but to differing degrees and levels of consequence. For example, software drivers for communication devices using copper subscriber lines, such voice band modems (V.90), asymmetric digital subscriber line (DSL) modems, home phone line networks (HomePNA), *etc.*, may be attacked, resulting in the subscriber line being disabled or improperly used. For example, a group of infected software modems may be used in a denial of service attack to continuously place calls to a predetermined number and overwhelm the destination. The software modem could also be used to prevent outgoing or incoming calls on the subscriber line or disrupt HomePNA traffic. Other wireless communication devices implemented in software, such as wireless network devices, could also be commandeered to disrupt traffic on the wireless network.

The present invention is directed to overcoming, or at least reducing the effects of, one or more of the problems set forth above.

SUMMARY OF THE INVENTION

One aspect of the present invention is seen in a communications system including a physical layer hardware unit and a processing unit. The physical layer hardware unit is adapted to communicate data over a communications channel in accordance with assigned transmission parameters. The physical layer hardware unit is adapted to receive an incoming signal over the communications channel and sample the incoming signal to generate a digital received signal. The processing unit is adapted to execute a standard mode driver in a standard mode of operation and a privileged mode driver in a privileged mode of operation.

The standard mode driver includes program instructions adapted to extract control codes from the digital received signal and configure the physical layer hardware assigned transmission parameters based on the control codes. The privileged mode driver includes program instructions adapted to independently extract secure control codes from the digital received signal, determine an operational characteristic of the physical layer hardware unit, and signal a security violation in response to the operational characteristic being inconsistent with the secure control codes.

Another aspect of the present invention is seen in a method for identifying security violations in a transceiver. The method includes receiving digital data over a communications channel in a standard processing mode of a processing unit; extracting control codes from the digital received signal in the standard mode of operation; configuring assigned transmission parameters of a physical layer hardware unit in the transceiver in the standard processing mode based on the control codes; transitioning the processing unit into a privileged processing mode of operation; extracting secure control codes from the digital received signal in the privileged processing mode; determining an operational characteristic of the physical layer hardware unit in the transceiver in the privileged processing mode; comparing the operational characteristic to the secure control codes in the privileged processing mode; and signaling a security violation in response to the operational characteristic being inconsistent with the secure control codes.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention may be understood by reference to the following description taken in conjunction with the accompanying drawings, in which like reference numerals identify like elements, and in which:

Figure 1 is a simplified block diagram of a communications system in accordance with one illustrative embodiment of the present invention;

Figure 2 is a simplified block diagram of an exemplary computer that embodies a user station in the communications system of Figure 1; and

Figure 3 is a simplified functional block diagram illustrating the interactions between the standard mode driver and the privileged mode driver in the computer of Figure 2 in one particular embodiment of the present invention.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and are herein described in detail. It should be understood, however, that the description herein of specific embodiments is not intended to limit the invention to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION OF SPECIFIC EMBODIMENTS

Illustrative embodiments of the invention are described below. In the interest of clarity, not all features of an actual implementation are described in this specification. It will of course be appreciated that in the development of any such actual embodiment, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which will vary from one implementation to another. Moreover, it will be appreciated that such a

development effort might be complex and time-consuming, but would nevertheless be a routine undertaking for those of ordinary skill in the art having the benefit of this disclosure.

Referring to Figure 1, a block diagram of a communications system 10 is provided. The communications system 10 includes a user station 20 in communication with a central station 30 over a communication channel 40. In the illustrated embodiment, the user station 20 is a mobile computing device using a software modem 50 to communicate in accordance with a wireless communication protocol, such as GSM. The central station 30 may be a shared base station capable of serving a plurality of subscribers. Although the invention is described as it may be implemented in a wireless environment, its application is not so limited. The teachings herein may be applied to other communication environments using software implemented communication protocols (*e.g.*, V.90, ADSL, HomePNA, Wireless LAN, *etc.*).

The user station 20 may comprise a variety of computing devices, such as a desktop computer, a notebook computer, a personal data assistant (PDA), *etc.* For purposes of illustration, the user station 20 is described as it may be implemented using a notebook computer. The software modem 50 may be installed as an internal resource. As will be appreciated by those of ordinary skill in the art, the software modem 50 includes a physical layer (PHY) 70 implemented in hardware and a protocol layer 80 implemented in software. For purposes of illustration, the functions of the software modem 50 are described as they might be implemented for a GSM communication protocol, although other protocols may be used.

The PHY layer 70 converts digital transmit signals into an analog transmit waveform and converts an incoming analog received waveform into digital received signals. For transmit signals, the output of the protocol layer 80 is the transmit "on-air" information

modulated about a zero Hz carrier (*i.e.*, a carrierless signal). The PHY layer 70 mixes (*i.e.*, mixing may also be referred to as upconverting) the carrierless transmit signal generated by the protocol layer 80 in accordance with assigned time slot, frequency, and power level assignments communicated to the user station 20 by the central station 30 to generate the actual analog waveform transmitted by the PHY layer 70.

The central station 30 also communicates time slot and frequency assignments to the user station 20 for incoming data. The incoming analog receive waveform is sampled and downconverted based on the assigned time slot and frequency parameters to recreate a carrierless (*i.e.*, modulated about zero Hz) receive waveform. The protocol layer 80 receives the carrierless receive waveform from the PHY layer 70 and performs baseband processing, decryption, and decoding to regenerate the received data.

Collectively, the time slot, frequency, and power level (*i.e.*, for transmit data only) assignments are referred to as control codes. The particular algorithms used for implementing the software modem 50 are described by the particular industry standards (*e.g.*, GSM standards) and are well known to those of ordinary skill in the art, so for clarity and ease of illustration they are not detailed herein, except as they are modified in accordance with the present invention.

In the communications system 10 of the instant invention, the central station 30 transmits data in accordance with traditional GSM techniques. The data received by the protocol layer 80 is encrypted. As described in greater detail below, the protocol layer 80 functions are divided into privileged mode functions and standard mode functions. The standard mode functions include decoding and decrypting the received data, extracting the control codes and user data, and sending the control codes to the PHY layer 70. The privileged mode functions include comparing the actual operational characteristics of the

PHY layer 70 with the assignments contained in the control codes to identify improper operation of the software modem 50 (*i.e.*, due to co-opting of the modem 50 by a software virus). If the privileged mode driver 250 determines that the PHY layer 70 is being operated inconsistently with its control code assignments, further operation of the software modem 50 and/or the user station 20 is inhibited.

Turning now to Figure 2, a block diagram of the user station 20 embodied in a computer 100 is provided. The computer 100 includes a processor complex 110. For clarity and ease of understanding not all of the elements making up the processor complex 110 are described in detail. Such details are well known to those of ordinary skill in the art, and may vary based on the particular computer vendor and microprocessor type. Typically, the processor complex 110 includes a microprocessor, cache memories, system memory, a system bus, a graphics controller, and other devices, depending on the specific implementation.

The processor complex 110 has two modes of operation, a standard mode and a privileged mode. An exemplary privileged mode of operation, well known to those of ordinary skill in the art, is the System Management Mode (SMM). Entry into the SMM is initiated through a system management interrupt (SMI). In response to an SMI, the processor complex 110 executes SMM code previously loaded (*i.e.*, during the initialization of the computer 100 and loading of the BIOS code) into a protected portion of the system memory not visible to any other processes (*e.g.*, applications or drivers). The memory locations used to perform the functions of the processor complex 110 during the SMM event are also not apparent to any other process. Although the illustrative embodiment is described as it may be implemented using SMM as a privileged mode, the invention is not so limited, and a different type of privileged mode may be used. In general, a privileged mode is defined as a mode of

operation not visible to other processes, such as applications or drivers, executing on the computer 100. SMM is simply one illustrative privileged mode currently available.

Other privileged contexts include the use of a separate processing entity, such as a cryptoprocessor, independent from the main system microprocessor. The functions of privileged mode software are executed by the cryptoprocessor and are thus secure from tampering by other software applications executing on the main system microprocessor. Still another privileged context is possible using a main system microprocessor having a secure architecture extension. In such an implementation, the cryptoprocessor is integrated into the main system microprocessor and controlled with secure commands.

The processor complex 110 is coupled to a peripheral bus 120, such as a peripheral component interface (PCI) bus. Typically a bridge unit (*i.e.*, north bridge) in the processor complex 110 couples the system bus to the peripheral bus 120. A south bridge 150 is coupled to the peripheral bus 120. The south bridge 150 interfaces with a low pin count (LPC) bus 160 that hosts a system basic input output system (BIOS) memory 170, a universal serial bus (USB) 180 adapted to interface with a variety of peripherals (*e.g.*, keyboard, mouse, printer, scanner, scanner) (not shown), an enhanced integrated drive electronics (EIDE) bus 190 for interfacing with a hard disk drive 200 and a CD-ROM drive (not shown), and an integrated packet bus (IPB) 210.

The IPB bus 210 hosts the hardware portion of the software modem 50. In the illustrated embodiment, the software modem 50 is hosted on an advanced communications riser (ACR) card 215. Specifications for the ACR card 215 and the IPB bus 210 are available from the ACR Special Interest Group (ACRSIG.ORG). The software modem 50 includes a PHY hardware unit 220 and a radio 230. In the illustrated embodiment, the radio 230 is

adapted to transmit and receive GSM signals. Collectively, the PHY hardware unit 220 and the radio 230 form the PHY layer 70 (see Figure 1).

The processor complex 110 executes program instructions encoded in a standard mode driver 240 and a privileged mode driver 250. The privileged mode driver 250 is loaded into the SMM space of the processor complex 110 during initialization of the computer 100. The privileged mode driver 250 may be stored in a secure location, such as the system BIOS 170, a secure memory device on the ACR card 215, a secure memory device in the computer 100, *etc.* An exemplary technique for storing a secure driver is described in U.S. Patent Application No. XX/XXX,XXX, (Attorney Docket No. 2000.053400/DIR, Client Docket No. TT4040), in the names of Terry L. Cole, David W. Smith, Rodney Schmidt, Geoffrey S. Strongin, Brian C. Barnes, and Michael Barclay, entitled, "PERIPHERAL DEVICE WITH SECURE DRIVER," and incorporated herein by reference in its entirety. Collectively, the processor complex 110 and the drivers 240, 250 implement the functions of the protocol layer 80 (see Figure 1).

Turning now to Figure 3, a simplified functional block diagram illustrating the interactions between the standard mode driver 240 and the privileged mode driver 250 in one particular embodiment of the present invention is shown. For incoming data received by the software modem 50, the standard mode driver 240 demodulates the carrier-less waveform to reconstruct encrypted data 260 received by the PHY hardware 220. The process for reconstructing the encrypted data 260 is well known to those of ordinary skill in the art, and is defined in industry GSM standards. For clarity and ease of illustration, the details of the reconstruction process are not included herein.

After reconstructing the encrypted data 260, the standard mode driver 240 decrypts the encrypted data 260 using the industry standard decryption techniques defined by the GSM

standards to generate decrypted data 270. The standard mode driver 240 decodes the decrypted data 270 and extracts control codes 280 and/or user data 290. The standard mode driver 240 passes the control codes to the PHY hardware 220. In turn, the PHY hardware 220 configures the radio 230 based on the assigned time slot, frequency, and power level information contained in the control codes 280.

Periodically, the privileged mode driver 250 is invoked (*e.g.*, using an SMI). The processor complex 110 transitions to privileged mode (*i.e.*, SMM) in response to the SMI and executes the privileged mode driver 250. The privileged mode driver 250 operates on the encrypted data 260 to independently generate secure decrypted data 300 and secure control codes 310. Various techniques exist for passing the encrypted data 260 to the privileged mode driver 250. In one embodiment, the standard mode driver 240 passes a pointer indicating the memory location of the encrypted data 260. In another embodiment, a portion of the system memory is designated as a shared mailbox for privileged mode activities. Applications operating in the standard mode, such as the standard mode driver 240, may place data in a designated inbox of the shared memory space, and applications running in the privileged mode, such as the privileged mode driver 250, may place data in a designated outbox of the shared memory space. The outbox may be designated as read-only for standard mode applications. An exemplary computer system having a shared mailbox for passing data between standard mode and privileged mode applications is described in U.S. Patent Application Serial No. XX/XXX,XXX, (Attorney Docket No. 2000.038700/LHI, Client Docket No. TT3760), in the names of Dale E. Gulick and Geoffrey S. Strongin, entitled "INTEGRATED CIRCUIT FOR SECURITY AND MANAGEABILITY," and incorporated herein by reference in its entirety.

The privileged mode driver 250 accesses the PHY hardware 220 to determine the operational characteristics of the radio 230. If the control codes 280 passed by the standard mode driver 240 have not been altered, the operational characteristics of the radio 230 will be consistent with the secure control codes 310. If the operational characteristics of the radio 230 are not consistent with the secure control codes 310, the privileged mode driver 250 may take a variety of protective actions. For example, the privileged mode driver 250 may inhibit operation of the software modem 50 by disabling up the standard mode driver 240 or by entirely disabling the computer 100 by initiating an unrecoverable error condition.

The particular technique for invoking the privileged mode driver 250 and the frequency at which it is invoked may vary. For example, the standard mode driver 240 may call the privileged mode driver 250 at a predetermined frequency (*e.g.*, every N frames up to and including every frame). In an alternative embodiment, the privileged mode driver 250 may be invoked periodically by another process independent of the standard mode driver 240. For example the operating system under which the computer 100 operates may include a timer that is used to periodically initiate an SMI to invoke the privileged mode driver 250. In another embodiment, security hardware including a secure timer may be included in the computer 100 for periodically invoking the privileged mode driver 250. For example, a restart timer 155, resident on the south bridge 150 may be used to periodically invoke the privileged mode driver 250 after a predetermined amount of time has elapsed. The particular operation of the restart timer 155 is described in greater detail in U.S. Patent Application Serial No. ________, incorporated above.

Once the privileged mode driver 250 is invoked, it uses the secure control codes 310 extracted from the secure decrypted data 300 to determine the expected operational state of the PHY hardware 220 and radio 230. There are various techniques by which the privileged

mode driver 250 might identify a security violation. For example, if the standard mode driver 240 has failed to provided updated encrypted data 260 to the privileged mode driver 250, a violation may be triggered. Synchronization signals embedded by the central station 30 in generating the encrypted data 260 for transmission may be extracted from the secure decrypted data 300 to determine such a failure.

One technique for checking the operational characteristics of the software modem 50 includes comparing the secure control codes 310 to the actual control codes 280 sent to the PHY hardware 220. The standard mode driver 240 might be required to write its control codes 280 to the shared mailbox, for example. The privileged mode driver 250 might also query the PHY hardware 220 to determine the control codes 280 sent by the standard mode driver 240. Another technique includes querying the PHY hardware 220 to determine the actual operating state of the radio 230 (*e.g.*, transmitting, silent, frequency, power level, etc.). If this operating state is not consistent with the secure control codes 310, a violation may be triggered.

The specific technique used to compare the actual operating state to the expected operating state may vary, depending on the particular implementation. A combination of the techniques may also be used. For example, on some iterations the control codes 280 generated by the standard mode driver 240 may be evaluated. On other iterations, the PHY layer 220 may be queried, and still on other iterations, the actual operating state of the radio 230 may be determined. Certain techniques may be less computationally taxing, and a combination of techniques may provide increased efficiency. A combination of techniques may also be used to identify different types of potential attacks. For example, the attacks might include co-opting of the standard mode driver 240 to alter the control codes 280; blocking the control codes 280 sent by the standard mode driver 240 and substituting other

10970.0850

control codes; preventing the standard mode driver 240 from passing updated encrypted data 260 to the privileged mode driver 250, *etc.* A combination of techniques, in lieu of one particular technique, may be more effective in identifying violations.

For data being transmitted by the software modem 50, the standard mode driver 240 handles all the data processing functions, including encoding, interleaving, burst assembly, encryption, and baseband processing to generate the carrier-less transmit waveform. The standard mode driver 240 passes the transmit waveform to the PHY hardware 220 and radio 230 for upconverting in accordance with the assigned time slot, frequency, and power level previously defined by the control codes 280.

By overseeing the operational characteristics of the software modem 50, attempts at surreptitious control of the modem 50 may be identified and stopped relatively quickly. As such, the potential for wide scale disruption of the communications network is reduced. The security of the software modem 50 is increased without sacrificing the flexibility and adaptability features inherent in its software implementation.

The particular embodiments disclosed above are illustrative only, as the invention may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. Furthermore, no limitations are intended to the details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope and spirit of the invention. Accordingly, the protection sought herein is as set forth in the claims below.